Fall 2022, Math 522: Week 2 Problem Set
Due: Friday, September 16th, 2022
Greatest Common Divisors and the Euclidean Algorithm

Discussion problems. The problems below should be worked on in class.

(D1) *Proving the Euclidean algorithm yields greatest common divisors.*

(a) Compare your answers to Preliminary Problem (P1). Then use the Euclidean algorithm to find $(522, 402)$ and verify you get the same answer.

(b) Have 2 different members of your group each choose a 3-digit positive integer, with no common digits. Use the Euclidean algorithm to find their greatest common divisor.

(c) Try to locate 2-digit numbers $a, b \in \mathbb{Z}$ so that using the Euclidean algorithm to compute (a, b) takes as many steps as possible.

(d) For each of the following a and b, find $d = (a, b)$ with the Euclidean algorithm, then locate $x, y \in \mathbb{Z}$ with $ax + by = d$.

(i) $a = 15, b = 12$
(ii) $a = 63, b = 12$
(iii) $a = 138, b = 63$
(iv) $a = 522, b = 402$

(e) Using your work in the previous part, devise a method to obtain x and y from the Euclidean algorithm (this is known as the *extended Euclidean algorithm*).

(f) Let $a, b \in \mathbb{Z}$ be arbitrary, and suppose applying the Euclidean algorithm to find $d = (a, b)$ takes exactly 4 steps. Write q_1, q_2, q_3, q_4 and r_1, r_2, r_3, r_4 for the quotient/remainder from each step (in particular, $r_4 = 0$ and $r_3 = d$). Find a formula for $x, y \in \mathbb{Z}$ such that $ax + by = d$ (your formula should be in terms of the q's and r's).

(g) Suppose in the previous part, the Euclidean algorithm took exactly 5 steps. Find an analogous formula for x and y. If the process were to take k steps, can you conjecture a closed form for x and y in terms of $q_1, q_2, \ldots, q_k$ and $r_1, r_2, \ldots, r_k$?

Homework problems. You must submit *all* homework problems in order to receive full credit.

Unless otherwise stated, $a, b, c, d, n \in \mathbb{Z}$ are arbitrary.

For this assigment only, do *not* use prime factorization in any of your arguments.

(H1) Use the Euclidean algorithm to find $d = \gcd(559, 234)$. Then use the extended Euclidean algorithm to find $x, y \in \mathbb{Z}$ with $599x + 234y = d$.

(H2) Prove that if $(a, b) = 1$, then $(a, b^n) = 1$ for all $a, b, n \in \mathbb{Z}$ with $n \geq 1$.

(H3) Fix $a, b, c \in \mathbb{Z}$. Prove the equation $ax + by = c$ has integer solutions if and only if $(a, b) \mid c$.

(H4) Determine whether each of the following statements is true or false. Prove each true statement, and give a counterexample for each false statement.

(a) If $\gcd(a, b) > 1$ and $\gcd(a, c) > 1$, then $\gcd(b, c) > 1$.

(b) If $a \mid (b + c)$ and $(b, c) = 1$, then $(a, b) = 1$ and $(a, c) = 1$.

Challenge problems. Challenge problems are not required for submission, but bonus points will be awarded for submitting a partial attempt or a complete solution.

(C1) Prove that $\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$ for all $a, b, c \in \mathbb{Z}$.